

## UNITED STATES DISTRICT COURT

for the  
Western District of WashingtonIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Target Facebook Account more particularly described  
in Attachment A

Case No. MJ19-372

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Target Facebook Account more particularly described in Attachment A, attached hereto and incorporated herein.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 249	Hate crime
18 U.S.C. § 2261A	Stalking
18 U.S.C. § 371	Conspiracy

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Ariana Kroshinsky attached hereto and incorporated herein by reference.

☒ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

  
Applicant's signature

Ariana Kroshinsky, FBI Special Agent  
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or  
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/09/2019

  
Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, U.S. Chief Magistrate Judge  
Printed name and title

**ATTACHMENT A**

**Target Account Facebook, Inc.**

1. This warrant applies to information associated with Facebook user ID of **100001140135702, with user name Wilz Christian Burberry**, that is stored at the premises owned, maintained, controlled, or operated by Facebook, Inc. located at 1601 Willow Road, Menlo Park, California.

## **ATTACHMENT B**

### **Facebook - Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information for the account described in Attachment A-2, is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the Facebook user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

of;

- (i) All information about the Facebook pages that the account is or was a “fan”

- (j) All past and present lists of friends created by the account;

- (k) All records of Facebook searches performed by the account;

- (l) All information about the user’s access and use of Facebook Marketplace;

- (m) The types of service utilized by the user;

- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (p) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that relates to the ongoing investigation of violations of Interstate Stalking (Title 18, United States Code, Sections 2261A(2)(A) and (2)(B), Conspiracy to Engage in Interstate Stalking (Title 18, United States Code, Section 371), and Hate Crime (Title 18, United States Code, Section 249) involving Christian Fredy Djoko and others known and unknown, and for the user ID identified on Attachment A, information pertaining to the following matters:

- (a) Any content including e-mails, messages, texts, photographs, visual images, documents, spreadsheets, address lists, contact lists or communications of any type which could be used to identify the user and or their location;

- (b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

(c) All subscriber records associated with the specified accounts, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number;

(d) Any and all other log records, including IP address captures, associated with the specified accounts; and

(e) Any records of communications between Facebook and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

STATE OF WASHINGTON           )  
  )         SS.  
COUNTY OF KING               )

## I. INTRODUCTION AND AGENT BACKGROUND

## II. PURPOSE OF AFFIDAVIT

2. More specifically, I am requesting a warrant for the **Target Facebook Account** in order to receive historical data and other records in order to ascertain the user's recent whereabouts when using the said accounts, which would assist the investigation in locating and securing evidence and instrumentalities related to criminal activity described and referenced herein and a criminal investigation occurring in this

1 judicial district. Further, the subjects' location is relevant to his/her participation in some  
2 of the acts committed against the victim.

3 3. Based on my training and experience and the facts as set forth in this  
4 affidavit, there is probable cause to believe that federal offenses of Interstate Stalking  
5 (Title 18, United States Code, Sections 2261A(2)(A) and (2)(B), Conspiracy to Engage in  
6 Interstate Stalking (Title 18, United States Code, Section 371), and Hate Crime (Title 18,  
7 United States Code, Section 249), have been and are being committed by persons known  
8 and unknown including the user of the **Target Facebook Account**, namely, Christian  
9 Fredy Djoko. There is also probable cause to search the information described in  
10 Attachment A for the items described in Attachments B to assist in obtaining possession  
11 of evidence, instrumentalities, contraband and fruits of these crimes.

12 4. The facts set forth in this Affidavit are based on my own personal  
13 knowledge; knowledge obtained from other individuals during my participation in this  
14 investigation, including other law enforcement personnel and computer scientists; review  
15 of documents and records related to this investigation; communications with others who  
16 have personal knowledge of the events and circumstances described herein; and  
17 information gained through my training and experience. Because this Affidavit is  
18 submitted for the limited purpose of establishing probable cause in support of the  
19 application for a warrant, it does not set forth each and every fact that I or others have  
20 learned during the course of this investigation.

### 21 III. JURISDICTION

22 5. This Court has jurisdiction to issue the requested warrant because it is "a  
23 court of competent jurisdiction," as defined by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A),  
24 2703(c)(1)(A), and 2711. Specifically, the Court is "a district court of the United States  
25 that – has jurisdiction over the offense[s] being investigated." 18 U.S.C. § 2711(3)(A)(i).



#### IV. RELEVANT BACKGROUND

6. On August 1, 2019, the Grand Jury returned a two-count Indictment charging Marie Christine Fanyo-Patchou, Rodrigue Fodjo Kamden, and Christian Fredy Djoko with Conspiracy to Engage in Cyberstalking, in violation of Title 18, United States Code, Section 371 (Count 1), and Interstate Cyberstalking, in violation of Title 18, United States Code, Sections 2 and 2261A(2)(A) and (2)(B) (Count 2). *See* Exhibit 1, *United States v. Fanyo-Patchou et al*, CR19-146JCC. Arrest warrants were issued for each of these defendants.

7. Defendant Fanyo-Patchou was arrested on August 6, 2019, and an initial appearance and detention hearing was held in the District of Maryland. She was detained pending transfer to the Western District of Washington for arraignment.

8. Notice of the Indictment and Arrest Warrants have been provided to counsel for defendants Kamden and Djoko. Djoko self-surrendered on August 8, 2019.

9. Defendants Kamden and Djoko were also charged in King County Superior Court with the crime of Malicious Harassment, in violation of Revised Code of Washington Section 9A.37.080. That case arises out of the same circumstances as the conduct outlined in the Indictment. After the return of the Indictment by the Grand Jury (Exhibit 1), the King County Prosecuting Attorney's Office obtained an order of dismissal without prejudice in the malicious harassment case.

#### V. PRESERVATION OF ACCOUNT AND PRIOR FACEBOOK SEARCH WARRANT

10. On December 21, 2018, I submitted an Application for Search Warrant, accompanied by an affidavit in support of the application, to seize and search three Facebook accounts, namely, accounts with UID 1279801734, UID 100023633720499, and UID 100002532176517. By this reference, I am incorporating as though fully restated herein my prior affidavit sworn to on December 21, 2018, before the Honorable Mary Alice Theiler, United States Magistrate Judge, as Exhibit 2 to this Affidavit, and hereinafter referred to as December Kroshinsky Affidavit.



1           11. As stated in the December Kroshinsky Affidavit, UID 1279801734 is  
2 Kamden's Facebook identification number, and UID 100002532176517 is Fanyo-  
3 Patchou's Facebook identification number. I confirmed that these UID numbers were for  
4 Kamden and Fanyo-Patchou when I received responsive digital data related to those  
5 UIDs from Facebook.

6           12. However, the responsive digital data for UID 100023633720499 was not  
7 for Djoko. I subsequently learned that the FBI employee who researched the Facebook  
8 account information for Djoko likely made a scrivener's error in documenting the UID of  
9 Djoko's Facebook account for inclusion into the December Kroshinsky Affidavit.  
10 Djoko's Facebook account has a user name of Wilz Christian Burberry. I have viewed  
11 the Facebook profile and public pages for Facebook account user name Wilz Christian  
12 Burberry and have seen numerous photographs of Djoko posted on this account, along  
13 with personal information about Djoko, confirming for me that this Facebook account is  
14 used by and belongs to Djoko. On August 7, 2019, I watched as an FBI Support  
15 Operations Specialist (SOS) navigated to the Facebook profile page for user name Wilz  
16 Christian Burberry. She pressed "Ctrl + U" that caused a new tab to open and this  
17 contained a large amount of miscellaneous text pertaining to the Wilz Christian Burberry  
18 profile page. To locate the UID within the resulting information, pressing "Ctrl + F"  
19 again and typing in "profileid" will highlight the Wilz Christian Burberry profile ID, that  
20 is, the user ID (UID). The UID is a long string of numbers. The SOS conducted these  
21 steps and verified that the UID for the Wilz Christian Burberry Facebook account is  
22 100001140135702.

23           13. On November 8, 2018, the FBI submitted a preservation request to  
24 Facebook for UID 100001140135702. I renewed this request for preservation of that  
25 account on August 8, 2019, to Facebook.  
26  
27  
28

## V. SUMMARY OF PROBABLE CAUSE

14. By this reference, I am incorporating as though fully restated herein the SUMMARY OF PROBABLE CAUSE stated in Exhibit 2, the December Kroshinsky Affidavit. I believe that the information stated in my prior affidavit sets forth probable cause to believe that the **Target Facebook Account** used by Djoko contains evidence, instrumentalities, contraband and fruits of the crimes that are charged in the Indictment and under continuing investigation.

15. In brief, between September 2018 through November 3, 2018, defendant Djoko, along with co-defendants Kamden and Fanyo-Patchou, used a variety of electronic communications applications, including Facebook and WhatsApp,<sup>1</sup> to harass and intimidate U.M.<sup>2</sup> See Exhibit 1, Indictment, and Exhibit 2, December Kroshinsky Affidavit. Djoko and U.M. are both from Cameroon, and are in the United States on F-1 student visa status.

16. For example, on or about November 1, 2018, Djoko, using WhatsApp, sent to Kamden, a photograph of an array of printed copies of photographs of Fanyo-Patchou with U.M., along with a printed copy of U.M.'s marriage certificate to his male husband. Djoko and Kamden then discussed, by online messaging, when to publish the material. Kamden confirmed, "I posted." See Exhibit 1, Indictment, Paragraph 17.

17. On or about October 16, 2018, Kamden, using WhatsApp, sent a text message to Djoko stating, "I will send you you can publish," along with a digital copy of a photograph of U.M. and his husband in a motel room with their pajamas. Djoko responded, "[I]t's already done on face." I believe that the term "face" as used by Djoko in this message refers to Facebook.

18. I have also examined the WhatsApp content contained in Kamden's cell phone, number 206-407-4936.<sup>3</sup> Much of the content in Kamden's WhatsApp account

<sup>1</sup> WhatsApp is a social media messaging application similar to Facebook, and is owned by Facebook.

<sup>2</sup> U.M. is referenced in the Indictment as John Doe.

<sup>3</sup> This cell phone number was a digital device authorized for search under the Court's previous Search Warrant, MJ18-584. Exhibit 2. The cell phone for Djoko was seized by Seattle Police Department officers when he was

1 relating to U.M. was also contained in Kamden's Facebook account (UID 1279801734).  
 2 I believe, similarly, that messaging and information about U.M. by Djoko using  
 3 WhatsApp will also likely be contained within Djoko's Facebook account, such as  
 4 photographs of U.M., personal information about U.M., and messaging to co-defendants  
 5 and other unidentified coconspirators about U.M.

## 6 **VII. BACKGROUND REGARDING FACEBOOK'S SERVICES**

7 19. Facebook, Inc. (hereafter Facebook) owns and operates a free-access social  
 8 networking website of the same name that can be accessed at <http://www.facebook.com>.  
 9 Facebook allows its users to establish accounts through which users can share written  
 10 news, photographs, videos, and other information with other Facebook users, and  
 11 sometimes with the general public.

12 20. Facebook asks users to provide basic contact information, either during the  
 13 registration process or thereafter. This information may include the user's full name,  
 14 birth date, contact e-mail addresses, physical address (including city, state, and zip code),  
 15 telephone numbers, screen names, websites, and other personal identifiers. Facebook  
 16 also assigns a user identification number to each account.

17 21. Facebook users can select different levels of privacy for the  
 18 communications and information associated with their Facebook accounts. By adjusting  
 19 these privacy settings, a Facebook user can make information in the user's account  
 20 available only to himself or herself, to other specified Facebook users, to all Facebook  
 21 users, or to anyone with access to the Internet, including people who are not Facebook  
 22 users. Facebook accounts also include other account settings that users can adjust to  
 23 control, for example, the types of notifications they receive from Facebook. Depending  
 24 on the user's privacy settings, Facebook may also obtain and store the physical location  
 25 of the user's device(s) as they interact with the Facebook service on those device(s).

26 \_\_\_\_\_  
 27 arrested on the state case, and it appeared that Djoko had deleted much of the content on the cell phone. For this  
 28 reason, law enforcement could not recover any content associated with Djoko's Facebook or WhatsApp accounts  
 from his cell phone for much of the time period in question.

1           22. Facebook users may join one or more groups or networks to connect and  
2 interact with other users who are members of the same group or network. A Facebook  
3 user can also connect directly with individual Facebook users by sending each user a  
4 “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two  
5 users will become “Friends” for purposes of Facebook and can exchange  
6 communications or view information about each other. Each Facebook user’s account  
7 includes a list of that user’s “Friends” and a “Mini-Feed,” which highlights information  
8 about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

9           23. Facebook users can create profiles that include photographs, lists of  
10 personal interests, and other information. Facebook users can also post “status” updates  
11 about their whereabouts and actions, as well as links to videos, photographs, articles, and  
12 other items available elsewhere on the Internet. Facebook users can also post information  
13 about upcoming “events,” such as social occasions, by listing the event’s time, location,  
14 host, and guest list. A particular user’s profile page also includes a “Wall,” which is a  
15 space where the user and his or her “Friends” can post messages, attachments, and links  
16 that will typically be visible to anyone who can view the user’s profile.

17           24. Facebook has a Photos application, where users can upload an unlimited  
18 number of albums and photos. Another feature of the Photos application is the ability to  
19 “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a  
20 photo or video, he or she receives a notification of the tag and a link to see the photo or  
21 video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by  
22 that user that have not been deleted, as well as all photos uploaded by any user that have  
23 that user tagged in them.

24           25. Facebook users can exchange private messages on Facebook with other  
25 users. These messages, which are similar to e-mail messages, are sent to the recipient’s  
26 “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well  
27 as other information. Facebook users can also post comments on the Facebook profiles  
28

1 of other users or on their own profiles; such comments are typically associated with a  
2 specific posting or item on the profile.

3 26. Facebook Notes is a blogging feature available to Facebook users, and it  
4 enables users to write and post notes or personal web logs (“blogs”), or to import their  
5 blogs from other services, such as Xanga, LiveJournal, and Blogger.

6 27. The Facebook Gifts feature allows users to send virtual “gifts” to their  
7 friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase,  
8 and a personalized message can be attached to each gift. Facebook users can also send  
9 each other “pokes,” which are free and simply result in a notification to the recipient that  
10 he or she has been “poked” by the sender.

11 28. In addition to the applications described above, Facebook also provides its  
12 users with access to thousands of other applications on the Facebook platform. When a  
13 Facebook user accesses or uses one of these applications, an update about that the user’s  
14 access or use of that application may appear on the user’s profile page.

15 29. Some Facebook pages are affiliated with groups of users, rather than one  
16 individual user. Membership in the group is monitored and regulated by the  
17 administrator or head of the group, who can invite new members and reject or accept  
18 requests by users to enter. Facebook can identify all users who are currently registered to  
19 a particular group and can identify the administrator and creator of the group. Facebook  
20 also assigns a group identification number to each group. Facebook uses the term  
21 “Group Contact Info” to describe the contact information for the group’s creator and  
22 administrator, as well as the current status of the group profile page.

23 30. Facebook uses the term “Neoprint” to describe an expanded view of a given  
24 user profile. The “Neoprint” for a given user can include the following information from  
25 the user’s profile: profile contact information; Mini-Feed information; status updates;  
26 links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists,  
27 including the friends’ Facebook user identification numbers; groups and networks of  
28 which the user is a member, including the groups’ Facebook group identification

1 numbers; future and past event postings; rejected “Friend” requests; comments; gifts;  
2 pokes; tags; and information about the user’s access and use of Facebook applications.

3 31. Facebook also retains IP address logs for a given user ID or IP address.  
4 These logs may contain information about the actions taken by the user ID or IP address  
5 on Facebook, including information about the type of action, the date and time of the  
6 action, and the user ID and IP address associated with the action.

7 32. Social networking providers like Facebook typically retain additional  
8 information about their users’ accounts, such as information about the length of service  
9 (including start date), the types of service used, and the means and source of any  
10 payments associated with the service (including any credit card or bank account number).  
11 In some cases, Facebook users may communicate directly with Facebook about issues  
12 relating to their account, such as technical problems, billing inquiries, or complaints from  
13 other users. Social networking providers like Facebook typically retain records about  
14 such communications, including records of contacts between the user and the provider’s  
15 support services, as well records of any actions taken by the provider or user as a result of  
16 the communications.

17 33. Therefore, the computers of Facebook are likely to contain all the material  
18 just described, including stored electronic communications and information concerning  
19 subscribers and their use of Facebook, such as account access information, transaction  
20 information, and account application.

## 21 **VIII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

22 34. Pursuant to Title 18, United States Code, Section 2703(g), this application  
23 and affidavit for search warrants seeks authorization to permit Facebook, Inc., and its  
24 agents and employees, to assist agents in the execution of this warrant. Once issued, the  
25 search warrant will be presented to Facebook, Inc., with direction that Facebook identify  
26 the account described in Attachments A to this affidavit, respectively, as well as other  
27 subscriber and log records associated with the account, as set forth in Section I of  
28 Attachments B to this affidavit.

1           35. The search warrant will direct Facebook, Inc. to create an exact copy of the  
2 specified account and records, including an exact copy of the contents of the hard disk  
3 drive or drives installed on the server associated with the **Target Facebook Account**, or  
4 the original drives.

5           36. I, and/or other law enforcement personnel will thereafter review the copy of  
6 the electronically stored data, and identify from among that content those items that come  
7 within the items identified in Section II to Attachment B, for seizure.

8           37. Analyzing the data contained in the forensic image may require special  
9 technical skills, equipment, and software. It could also be very time-consuming.  
10 Searching by keywords, for example, can yield thousands of “hits,” each of which must  
11 then be reviewed in context by the examiner to determine whether the data is within the  
12 scope of the warrant. Merely finding a relevant “hit” does not end the review process.  
13 Keywords used originally need to be modified continuously, based on interim results.  
14 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,  
15 search text, and many common e-mail, database and spreadsheet applications do not store  
16 data as searchable text. The data may be saved, instead, in proprietary non-text format.  
17 And, as the volume of storage allotted by service providers increases, the time it takes to  
18 properly analyze recovered data increases, as well. Consistent with the foregoing,  
19 searching the recovered data for the information subject to seizure pursuant to this  
20 warrant may require a range of data analysis techniques and may take weeks or even  
21 months. All forensic analysis of the data will employ only those search protocols and  
22 methodologies reasonably designed to identify and seize the items identified in Section II  
23 of Attachment B to the warrant.

#### 24                               IX. REQUEST FOR SEALING

25           38. I further request this Court issue an order sealing, until further order of the  
26 Court, all papers submitted in support of the requested search warrant, including the  
27 application, this affidavit, the attachments, and the requested search warrant. I believe  
28 sealing these documents is necessary because the information to be seized is relevant to



1 an ongoing investigation, and any disclosure of the information at this time may cause  
2 Djoko and his co-defendants, Kamden and Fanyo-Patchou, or others as yet unidentified  
3 coconspirators, to flee from prosecution, cause destruction of or tampering with evidence,  
4 or otherwise seriously jeopardize this investigation. Premature disclosure of the contents  
5 of the application, this affidavit, the attachments, and the requested search warrant may  
6 adversely affect the integrity of the investigation. Further, an Order Sealing the Search  
7 Warrant (Exhibit 2) was authorized by Magistrate Judge Theiler.

## 8 X. CONCLUSION

9 39. Based on the foregoing, I believe evidence of probable cause has been  
10 established that evidence, instrumentalities, contraband and fruits of violations of the  
11 federal crimes of Interstate Stalking (Title 18, United States Code, Sections 2261A(2)(A)  
12 and (2)(B), Conspiracy to Engage in Interstate Stalking (Title 18, United States Code,  
13 Section 371), and Hate Crime (Title 18, United States Code, Section 249), are located in  
14 the **Target Facebook Account** as more fully described in Attachment A to this Affidavit.

15 40. I request that the Court issue the proposed search warrant, pursuant to  
16 Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I further request that the  
17 Court authorize execution of the warrant at any time of day or night, owing to the  
18 potential need to locate the **Target Facebook Account** outside of daytime hours.  
19 Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not  
20 required for the service or execution of this warrant. Accordingly, by this Application  
21 and Affidavit, I seek authority for the government to search all of the items specified in  
22 Section I of Attachment B (attached hereto and incorporated by reference herein) to the  
23 Warrant, and specifically to seize all of the data, documents and records that are  
24 identified in Section II to that same Attachment.

25 41. I further request that the Court direct Provider to disclose to the government  
26 any information described in Attachment B that is within the possession, custody, or  
27 control of Provider. I also request that the Court direct Provider to furnish the  
28 government all information, facilities, and technical assistance necessary to accomplish

1 the collection of the information described in Attachment B unobtrusively and with a  
2 minimum of interference with Provider's services, including by initiating a signal to  
3 determine the location of the **Target Facebook Account** on provider's network or with  
4 such other reference points as may be reasonably available, and at such intervals and  
5 times directed by the government.

6 I declare under the penalty of perjury that the statements above are true and correct  
7 to the best of my knowledge and belief.

8 DATED this 8 day of August, 2019.



ARIANA KROSHINSKY  
Special Agent  
Federal Bureau of Investigations

14  
15 SUBSCRIBED AND SWORN before me this on this 9 day of August 2019



BRIAN A. TSUCHIDA  
United States Chief Magistrate Judge

# EXHIBIT 1

Presented to the Court by the foreman of the  
Grand Jury in open Court, in the presence of  
the Grand Jury and FILED in the U.S.  
DISTRICT COURT at Seattle, Washington.

August 1 2019  
By William M. McCool, Clerk  
[Signature] Deputy

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,  
Plaintiff

v.

MARIE CHRISTINE FANYO-PATCHOU,  
RODRIGUE FODJO KAMDEN, and,  
CHRISTIAN FREDY DJOKO,  
Defendants.

NO **CR 19-146** JCC

INDICTMENT

The Grand Jury alleges that:

**General Allegations**

At all times material to this Indictment:

1. Defendants MARIE CHRISTINE FANYO-PATCHOU, RODRIGUE FODJO KAMDEN, and CHRISTIAN FREDY DJOKO were from Cameroon, a country in West Africa. John Doe was also from Cameroon. The defendants and John Doe lived in the United States during the years 2017 and 2018.

2. According to the U.S. Department of State's Cameroon 2018 Human Rights Report, in Cameroon, consensual same-sex sexual activity is illegal and punishable by imprisonment for a term lasting between six months and five years. The Report further describes that members of the Lesbian, Bisexual, Gay, Transgender, and

1 Queer community in Cameroon are routinely targeted for violence and threats of violence  
2 because of their real or perceived sexual orientation or gender identity.

3 3. John Doe is gay. He relocated to the United States in or around 2014.  
4 While in the United States, John Doe met his husband and they married in approximately  
5 2016.

### 6 COUNT 1

#### 7 **(Conspiracy to Engage in Cyberstalking)**

8 4. The allegations contained in Paragraphs 1 through 3 of this Indictment are  
9 re-alleged and incorporated into Count 1 as if set forth fully herein.

10 5. Beginning at a time unknown and within the last five years, and continuing  
11 through on or about November 3, 2018, in King and Snohomish Counties, within the  
12 Western District of Washington, and elsewhere, MARIE CHRISTINE FANYO-  
13 PATCHOU, RODRIGUE FODJO KAMDEN, CHRISTIAN FREDY DJOKO, and others  
14 known and unknown to the Grand Jury, conspired and agreed together to, with the intent  
15 to harass and intimidate John Doe, use an interactive computer service, an electronic  
16 communications service, an electronic communication system of interstate commerce,  
17 and other facilities of interstate and foreign commerce, to wit: text messages, online  
18 postings, and social media messaging and posting, including WhatsApp and Facebook, to  
19 engage in a course of conduct that:

20 a. Placed John Doe in reasonable fear of serious bodily injury to John  
21 Doe and John Doe's immediately family members, and,

22 b. Caused, attempted to cause, and would be reasonably expected to  
23 cause substantial emotional distress to John Doe and John Doe's immediate family  
24 members,

25 in violation of Title 18, United States Code, Sections 2261A(2)(A) and (2)(B).

### 26 MANNER AND MEANS OF THE CONSPIRACY

27 6. MARIE CHRISTINE FANYO-PATCHOU, RODRIGUE FODJO  
28 KAMDEN, CHRISTIAN FREDY DJOKO, and other co-conspirators, carried out the

1 conspiracy through the use of a variety of electronic communication applications,  
2 including Facebook and WhatsApp, through which they harassed and intimidated John  
3 Doe by distributing and disseminating personal and intimate materials relating to John  
4 Doe's sexual orientation to other members of the Cameroonian communities in the  
5 United States and Cameroon, and made threatening statements designed to place John  
6 Doe and his family members in fear of serious bodily injury.

7  
8 OVERT ACTS

9 During and in furtherance of the conspiracy, within the Western District of  
10 Washington and elsewhere, one or more of the following overt acts, among others, were  
11 committed:

12 7. During September 2018, FANYO-PATCHOU moved out of John Doe's  
13 residence and took with her a cell phone that contained copies of John Doe's personal  
14 photographs that documented his marriage and relationship to a man. Some of the  
15 photographs on the cell phone of John Doe were intimate in nature and contained nudity.

16 8. On or about October 4, 2018, in a WhatsApp messaging exchange,  
17 KAMDEN asked FANYO-PATCHOU to send him all the materials that she had  
18 pertaining to John Doe.

19 9. Between on or about October 16, 2018, and October 18, 2018, FANYO-  
20 PATCHOU used WhatsApp to send photographs and materials about John Doe and his  
21 husband to KAMDEN. These photographs and materials included a copy of John Doe's  
22 marriage certificate, a photograph of John Doe kissing his husband, a photograph of John  
23 Doe and his husband in a hotel room, and a nude photograph of John Doe.

24 10. Between on or about October 16, 2018, and November 3, 2018,  
25 KAMDEN uploaded the same photographs sent to him by FANYO-PATCHOU in at  
26 least one publicly available post over Facebook. KAMDEN further disseminated the  
27 photographs to other persons in the Cameroonian community, using text message and  
28 various social media platforms, including WhatsApp and Facebook.

11. For example, on or about October 17, 2018, KAMDEN, using WhatsApp,

1 communicated with “Chao” and sent several photographs of John Doe with his husband.  
2 These included photographs of John Doe and his husband kissing, the biographic page of  
3 John Doe’s passport, and John Doe’s Facebook Messenger contact profile. KAMDEN  
4 had previously obtained the biographic page of John Doe’s passport from DJOKO, who  
5 previously sent it to KAMDEN using WhatsApp on or about September 28, 2018.

6 12. On or about October 21, 2018, as part of the defendants’ course of conduct  
7 to place John Doe in fear of serious bodily injury, KAMDEN and DJOKO physically  
8 assaulted John Doe. During the assault, KAMDEN and DJOKO, in French, called John  
9 Doe a “faggot,” stated, “she tried to make you change but you didn’t want to,” (referring  
10 to FANYO-PATCHOU), and made other derogatory comments about John Doe’s sexual  
11 orientation.

12 13. On or about October 25, 2018, FANYO-PATCHOU, using Facebook,  
13 publicly posted this statement referring to John Doe: “The faggot of Seattle needs to kill  
14 himself after writing his will.”

15 14. In October 2018, John Doe received a WhatsApp message from an  
16 unknown co-conspirator using a phone number with a Cameroonian country code. The  
17 message stated, “[John Doe] will you really never change? Fanyo told us she did  
18 everything in the world to change you to make you hetero. You’re still remaining a  
19 faggot? Here’s your faggot direct from Fanyo.” The message included a photograph of  
20 John Doe with his husband. This was one of the photographs on the cell phone taken by  
21 FANYO-PATCHOU that she had also sent to KAMDEN using WhatsApp.

22 15. In October 2018, John Doe received a message on WhatsApp from another  
23 unknown co-conspirator with a phone number with a Cameroonian country code. The  
24 message stated: “[John Doe] we have your skin. Did you think you could run away from  
25 Cameroon to bake? You can’t escape, Fanyo is in the United States and we will do  
26 everything to destroy your marriage. You saw what we did to your mom’s house? It’s  
27 just the beginning. A faggot family from the father to the children. We have your  
28



1 address. We'll finish you." At that time, John Doe was aware of a recent incident  
2 involving the vandalism of his mother's home in Cameroon.

3 16. In and around early November 2018, KAMDEN published information on  
4 Facebook stating that John Doe is gay and falsely stating that John Doe was  
5 "prostituting" himself in the United States to make money.

6 17. On or about November 1, 2018, DJOKO, using WhatsApp, sent to  
7 KAMDEN a photograph of an array of printed copies of photographs of FANYO-  
8 PATCHOU with John Doe, along with a printed copy of John Doe's marriage certificate.  
9 DJOKO and KAMDEN then discussed when to publish this material, and KAMDEN  
10 confirmed, "I posted."

11 18. On or about November 1, 2018, KAMDEN, using WhatsApp, sent a text  
12 message to DJOKO stating, "I will send you you can publish," along with a digital copy  
13 of a photograph of John Doe and his husband in a motel room in their pajamas. DJOKO  
14 responded "[I]t's already done on face," referring to having posted the photo on  
15 Facebook.

16 19. On or about October 31, 2018, KAMDEN, using WhatsApp, sent a  
17 message to John Doe's stepmother who resides in Cameroon. The message was a screen  
18 shot of a photograph gallery that contained images of John Doe with his husband and a  
19 nude photograph of John Doe.

20 20. On or about November 2, 2018, KAMDEN, using WhatsApp, sent another  
21 message to John Doe's stepmother. This message was a screenshot of KAMDEN's  
22 Facebook page that contained a post stating John Doe "was a homosexual," and falsely  
23 stating "that he prostituted himself for money," and that he was physically abusive  
24 toward FANYO-PATCHOU, after which she became "infected with a STD."

25 21. Also on November 2, 2018, KAMDEN, using WhatsApp, sent to John  
26 Doe's father photographs of John Doe, including intimate photographs of John Doe and  
27 his husband.

28 All in violation of Title 18, United States Code, Section 371.

**COUNT 2**

**(Interstate Stalking)**

22. The allegations contained in Paragraphs 1-3, and 7-21 of this Indictment are re-alleged and incorporated into Count 2 as if set forth fully herein.

23. Beginning in or about September 2018, and continuing through on or November 3, 2018, in King and Snohomish Counties, within the Western District of Washington, and elsewhere, MARIE CHRISTINE FANYO-PATCHOU, RODRIGUE FODJO KAMDEN, and CHRISTIAN FREDY DJOKO, with the intent to harass and intimidate John Doe, used, and aided and abetted the use of, an interactive computer service, an electronic communication service, and electronic communication system of interstate commerce, and other facilities of interstate and foreign commerce, to wit: text messages, online postings, and social media messaging and posting, including WhatsApp and Facebook, to engage in a course of conduct that:

a. Placed John Doe in reasonable fear of serious bodily injury to John Doe and John Doe's immediately family members, and,

b. Caused, attempted to cause, and would be reasonably expected to cause substantial emotional distress to John Doe and John Doe's immediate family members.

24. The Grand Jury alleges that this offense was committed during and in furtherance of the conspiracy charged in Count 1 above.


1 All in violation of Title 18, United States Code, Sections 2 and 2261A(2)(A)  
2 and (2)(B).


3 A TRUE BILL.

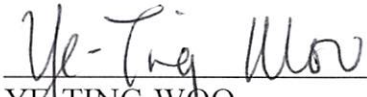
4 DATED: August 1, 2019


5 *Signature of the foreperson is redacted*  
6 *pursuant to the policy of the Judicial*  
7 *Conference of the United States*

FOREPERSON

8   
9  
10 BRIAN T. MORAN  
11 United States Attorney

12   
13 TODD GREENBERG  
14 Assistant United States Attorney

15  
16   
17 YE-TING WOO  
18 Assistant United States Attorney

19  
20   
21 FRANK LIN  
22 Senior Counsel  
23 Computer Crime and Intellectual Property Section  
24 U.S. Department of Justice  
25  
26  
27  
28

# EXHIBIT 2

DEC 21 2018

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

AT SEATTLE  
CLERK OF DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Target Cell Phone, Target Facebook Accounts, & Target  
Google Accounts more particularly described in  
Attachments A1, A2 & A3

Case No.

MJ18-584

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Target Cell Phone, Target Facebook Accounts, & Target Google Accounts more particularly described in Attachments A1, A2 & A3, attached hereto and incorporated herein.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachments B1, B2, & B3 hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

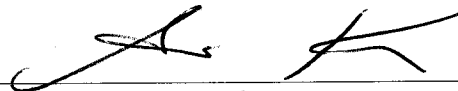
- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 249	Hate Crimes
18 USC 2261A	Stalking
18 USC 371	Conspiracy

The application is based on these facts:  
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: 02/03/2019) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Ariana Kroshinsky, Special Agent, FBI.

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/21/2018

City and state: Seattle, Washington

USAO #2018R01525



Judge's signature

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

1 **AFFIDAVIT**

2 STATE OF WASHINGTON )  
 3 ) ss  
 4 COUNTY OF KING )

5 I, Ariana Kroshinsky, having been duly sworn, state as follows:

6 **I. INTRODUCTION AND AGENT BACKGROUND**

7 2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and  
 8 have been since May 2018. I am presently assigned to a squad in the Seattle Field Office  
 9 that covers civil rights crimes. My training and experience includes investigations of  
 10 various federal criminal violations, including hate crimes and internet crimes. I have  
 11 attended the Federal Bureau of Investigation Special Agent Training Course. I have  
 12 participated in several hate crimes and internet crimes investigations, including  
 13 conducting physical surveillance and executing search warrants.

14 **II. PURPOSE OF AFFIDAVIT**

15 3. I make this affidavit in support of an application for search warrants under  
 16 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), to acquire information  
 17 associated with the following accounts that are stored at premises controlled by an  
 18 electronic communications service and remote computer service provider, namely:

- 19 a. **T-Mobile Wireless**, a wireless telephone service provider headquartered at  
 20 3625 132nd Ave SE, Bellevue, WA 98006, for information about the historical  
 21 location from October 20, 2018 through October 27, 2018, of the cellular  
 22 telephone assigned call number 206-407-4936, hereinafter "**Target Cell**  
 23 **Phone**";
- 24 b. **Facebook, Inc.** located at 1601 Willow Road, Menlo Park, California, to  
 25 search the following accounts: UID: 1279801734; UID: 100023633720499;  
 26 and UID: 100002532176517, hereafter "**Target Facebook Accounts**," and  
 27 disclose to the government all content, call logs, and messages sent and  
 28

received on the **Target Facebook Accounts**, as more fully described in Attachment A2.

c. **Google, Inc.**, located at 1600 Amphitheatre Parkway, Mountain View, California 94043, to search for and provide Google + Accounts: UID: 117906598794476810352, hereafter **Target Google Account** for any data, content, logs, log in, and any data backed up and stored from third party accounts on the **Target Google Account**.

4. More specifically, I am requesting warrants for the **Target Cellphone, Facebook, and Google Accounts**, in order to receive historical data and other records in order to ascertain the user's recent whereabouts when using the said accounts, which would assist the investigation in locating and securing evidence and instrumentalities related to criminal activity described and referenced herein and a criminal investigation occurring in this judicial district. Further, the subjects' location is relevant to his/her participation in some of the acts committed against the victim.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections: 249 (hate crimes), 2261A (stalking), and 371 (conspiracy), have been and are being committed by persons known and unknown including the user of the **Target Cellphone, Facebook, and Google Accounts**, namely, Marie Christine Fanyo-Patcho, Rodrigue Fodjo Kamden and Christian Fredy Djoko. There is also probable cause to search the information described in Attachments A1-3 for the items described in Attachments B1-3 to assist in obtaining possession of evidence, instrumentalities, contraband or fruits of these crimes.

6. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel and computer scientists; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and



1 information gained through my training and experience. Because this Affidavit is  
2 submitted for the limited purpose of establishing probable cause in support of the  
3 application for a warrant, it does not set forth each and every fact that I or others have  
4 learned during the course of this investigation.

### 5 **III. JURISDICTION**

6 7. This Court has jurisdiction to issue the requested warrant because it is “a  
7 court of competent jurisdiction,” as defined by 18 U.S.C. §§ 18 U.S.C. §§ 2703(a),  
8 2703(b)(1)(A), 2703(c)(1)(A), and 2711. Specifically, the Court is “a district court of the  
9 United States that – has jurisdiction over the offense[s] being investigated.” 18 U.S.C.  
10 § 2711(3)(A)(i).

### 11 **IV. SUMMARY OF PROBABLE CAUSE**

12 8. The victim, U.M., and subjects of the investigation, Rodrigue Fodjo  
13 Kamden (hereafter “Kamden”), Christian Fredy Djoko (hereafter “Djoko”), and Marie  
14 Christine Fanyo-Patcho (hereafter “Fanyo-Patcho”), are all from Cameroon, a country  
15 located in West Africa. The official languages are French and English, though French is  
16 the primary language spoken. Christianity is the dominate faith. According to the U.S.  
17 Department of State’s Cameroon 2017 Human Rights Report, in Cameroon  
18 homosexuality is illegal and can result in imprisonment from 6 months up to five years  
19 and fines of \$37-373. Members of the LBGT community in Cameroon are often targeted  
20 for threats and harassment.

21 9. Between approximately September 2018, through November 2018,  
22 following a disagreement between U.M. and Fanyo-Patcho, the subjects began seeking to  
23 harass, embarrass, and humiliate U.M. by posting and texting personal and intimate  
24 content about U.M.’s sexual preference to other members of the Cameroon community as  
25 well as U.M.’s family members. The subjects used Facebook, WhatsApp, and Google +  
26 to post this information and communicate with one another and others.

1           10.     In approximately 2014, U.M. came to the United States on a student visa to  
2 attend school. Sometime after he arrived in the Seattle area, U.M. became involved in a  
3 relationship with another man and in approximately 2016, the two were married.

4           11.     In approximately December 2017, Marie Christine Fanyo-Patchou (Fanyo-  
5 Patchou), a friend of U.M. from Cameroon, came to visit him and stayed in his  
6 apartment. According to U.M. while they were living in Cameroon and attending high  
7 school, he had disclosed to Fanyo-Patchou that he was gay. Before Fanyo-Patchou came  
8 to visit, U.M. had told her that he had gotten married to a man.

9           12.     After Fanyo-Patchou began living with U.M., she constantly told him that  
10 being gay was not right and tried to convince him to be heterosexual. Fanyo-Patchou  
11 offered to help U.M. become heterosexual by having sexual intercourse with him. At one  
12 point Fanyo-Patchou asked him what he thought would happen if members of the  
13 Cameroon community learned he was gay and had a husband.

14           13.     In late September 2018, U.M. told Fanyo-Patchou that she could no longer  
15 live in his residence. Fanyo-Patchou went to stay with another associate of hers, Rodrigue  
16 Fodjo Kamden (Kamden). Unbeknownst to U.M., when Fanyo-Patchou moved out, she  
17 took a cell phone that U.M. had given her to use. On the phone were intimate  
18 photographs of U.M. with his husband. Further, while living with U.M., she had secretly  
19 taken photos of U.M.'s personal photograph collection that documented his marriage.  
20 Some of the photographs that Fanyo-Patchou copied were private and contained nudity.

21           14.     After moving in with Kamden, Fanyo-Patchou shared the photographs of  
22 U.M. and his husband with Kamden and another associate, Christian Fredy Djoko  
23 (Djoko). Shortly thereafter, Kamden and Djoko began releasing the photographs of U.M.  
24 and his husband online to members of Cameroon community via text message, the  
25 Google + platform of Whatsapp, and Facebook. After the photographs of U.M. were  
26 posted online, U.M. stated that he started receiving threatening texts and voicemail  
27 messages from unknown numbers with the Cameroonian country code.  
28

1           15.     On October 22, 2018, U.M. called 911 to report that he had been assaulted.  
2     Seattle Police Officer, Joshua Brilla, responded. Officer Brilla met with U.M. who  
3     reported that on October 21, 2018, at approximately 1:00 A.M., he had parked his car and  
4     was walking toward his residence when he was approached by two Cameroonian men  
5     who called out to him in French using Cameroonian slang. U.M. has subsequently  
6     identified the men as Kamden and Djoko. U.M. stated that Djoko grabbed him from  
7     behind and pulled his wrists behind his back while Kamden grabbed his ears and pulled  
8     him to his knees. U.M. stated that the men were squeezing him and were calling him  
9     “faggot” and making other derogatory comments about his sexual orientation. U.M. also  
10    reported that the men said, “she tried to make you change but you didn’t want to.” U.M.  
11    interpreted this to mean that Fanyo-Patcho had tried to convert him to be heterosexual but  
12    he didn’t convert.

13           16.     After the assault ended U.M. returned to his residence. Later in the  
14    morning he called his brother and told him what happened. The following day he called  
15    a gay rights support service who urged him to report the attack to the police, which he did  
16    on Monday, October 22, 2018. Officer Brilla noted that U.M. suffered injuries/bruising  
17    to his ears and knees.

18           17.     In subsequent interviews with law enforcement, U.M. has disclosed that the  
19    men were armed with a kitchen knife and that in addition to physically grabbing him, that  
20    Kamden forced his penis into U.M.’s mouth.

21           18.     On October 25, 2018, U.M. reported to the Seattle Police that Fanyo-  
22    Patchou posted on her Facebook page in French that, “the faggot of Seattle needs to kill  
23    himself after writing his will” which U.M. interpreted as referring to him. Kamden  
24    responds “don’t worry it’s in the process. I already told you not to go that way. You will  
25    lose.”

26           19.     U.M. also received texts from mobile number (206) 407-4936 (**Target Cell**  
27    **Phone**) which he believed to be Kamden’s mobile phone. One of the messages stated  
28    that U.M. needed to calm down or his “faggot husband photos would be posted online.”

1 Another text from the **Target Cell Phone** referenced that U.M. should not have tried to  
2 serve him papers (U.M. had Kamden and Djoko both served with anti-harassment  
3 orders). U.M. said he also received three phone calls from the **Target Cell Phone** but he  
4 did not answer them (a search of the Accurant database showed (206) 407-4936 is a T-  
5 Mobile account belonging to Rodrigue Fodjo Kamden of Lynnwood, Washington).  
6 These phone calls violated the anti-harassment order.

7 20. U.M. has seen postings that Kamden and Djoko have posted on Facebook,  
8 to which they attached sexual photos of U.M., announcing that U.M. is gay and  
9 “prostituting” himself in America to make money. Multiple relatives of U.M. have told  
10 him that Kamden has texted them the photographs.

11 21. On November 2, 2018, U.M. reported that unknown persons spray-painted  
12 his vehicle with the words, “Dirty” and “Fag” and images in the shape of penises.

13 22. I learned that Kamden’s Facebook user account identification is  
14 1279801734 and that his Google+ account identification is 117906598794476810352.

15 23. I have learned that Djoko’s Facebook account identification is  
16 100023633720499, his Google + account information is 114036295919816718188.

17 24. Fanyo-Patchou’s Facebook Account is 100002532176517.

18 25. Because Kamden and Djoko are both frequent users of text messaging and  
19 social media including Facebook, WhatsApp, and Google +, I believe that the  
20 geolocation data requested is relevant and material to the ongoing criminal investigation  
21 and will likely reveal fruits, contraband, instrumentalities, or evidence of violation of  
22 Title 18, United States Code, Sections of 249 (hate crimes), 370 (conspiracy) and 2261A  
23 (Stalking).

24 26. On November 3, 2018, Kamden and Djoko were arrested for the assault on  
25 U.M. Kamden’s phone, (206) 407-4936 (**Target Cell Phone**) was taken from Kamden.  
26 On or about November 5, 2018, Kamden was released from custody when charges were  
27 not formally filed.  
28

27. Detective Tim DeVore of the Seattle Police Department obtained a search warrant to search the **Target Cell Phone**. I have reviewed the contents of the **Target Cell Phone**. In reviewing the photos and text messages copied from Kamden's phone by the Seattle Police Department, I learned that Kamden frequently used WhatsApp and had taken screenshots of some of his WhatsApp and text message conversations, including conversations with Cameroonian phone numbers to which he sent the pictures of U.M. Kamden had multiple copies of the pictures of U.M., including the photos taken by Fanyo-Patchou from U.M.'s hardcopy photo albums, photos in his tablet, and photos of his marriage certificate. There was a screenshot of a conversation between Kamden and "Marie de Seattle" (whom I believe to be Fanyo-Patchou) in which Fanyo-Patchou texted the photos of U.M. to Kamden. Also on Kamden's phone was a screenshot of a text message conversation that had taken place between U.M. and Djoko where U.M. revealed he was gay. There was a screenshot of a WhatsApp conversation between Kamden and U.M.'s father showing that Kamden sent him the photos, U.M.'s marriage certificate, and a photo of a sexual conversation U.M. had with another man on his tablet. There was a screenshot of a Facebook post Kamden had made describing U.M. as gay.

## Target Cell Phone

28. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone services have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some

1 cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These  
2 towers are often a half-mile or more apart, even in urban areas, and can be 10 or more  
3 miles apart in rural areas. Furthermore, the tower closest to a wireless device does not  
4 necessarily serve every call made to or from that device. Accordingly, cell-site data is  
5 typically less precise than E-911 Phase II data.

6 29. Based on my training and experience, I know that providers of cell service  
7 such as T-Mobile can collect E-911 Phase II data about the location of the **Target Cell**  
8 **Phone**, including by initiating a signal to determine the location of the **Target Cell**  
9 **Phone** on the provider’s network or with such other reference points as may be  
10 reasonably available.

11 30. Based on my training and experience, I know that providers such as T-  
12 Mobile can collect cell-site data about the **Target Cell Phone**.

13 31. In my training and experience, I have learned that cellular phones and other  
14 cellular devices communicate wirelessly across a network of cellular infrastructure,  
15 including towers that route and connect individual communications. When sending or  
16 receiving a communication, a cellular device broadcasts certain signals to the cellular  
17 tower that is routing its communication. These signals include a cellular device’s unique  
18 identifiers.

19 32. I believe the collection of E-911 Phase II data and cell-site data related to  
20 the **Target Cell Phone** has relevant information related to the crimes against U.M.  
21 Specifically, it will show the location of the **Target Cell Phone** on the date that U.M.  
22 was assaulted.

### 23 Facebook Technical Background

24 33. Facebook, Inc. (hereafter Facebook) owns and operates a free-access social  
25 networking website of the same name that can be accessed at <http://www.facebook.com>.  
26 Facebook allows its users to establish accounts through which users can share written  
27 news, photographs, videos, and other information with other Facebook users, and  
28 sometimes with the general public.

1       34. Facebook asks users to provide basic contact information, either during the  
2 registration process or thereafter. This information may include the user's full name,  
3 birth date, contact e-mail addresses, physical address (including city, state, and zip code),  
4 telephone numbers, screen names, websites, and other personal identifiers. Facebook  
5 also assigns a user identification number to each account.

6       35. Facebook users can select different levels of privacy for the  
7 communications and information associated with their Facebook accounts. By adjusting  
8 these privacy settings, a Facebook user can make information in the user's account  
9 available only to himself or herself, to other specified Facebook users, to all Facebook  
10 users, or to anyone with access to the Internet, including people who are not Facebook  
11 users. Facebook accounts also include other account settings that users can adjust to  
12 control, for example, the types of notifications they receive from Facebook. Depending  
13 on the user's privacy settings, Facebook may also obtain and store the physical location  
14 of the user's device(s) as they interact with the Facebook service on those device(s).

15       36. Facebook users may join one or more groups or networks to connect and  
16 interact with other users who are members of the same group or network. A Facebook  
17 user can also connect directly with individual Facebook users by sending each user a  
18 "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two  
19 users will become "Friends" for purposes of Facebook and can exchange  
20 communications or view information about each other. Each Facebook user's account  
21 includes a list of that user's "Friends" and a "Mini-Feed," which highlights information  
22 about the user's "Friends," such as profile changes, upcoming events, and birthdays.

23       37. Facebook users can create profiles that include photographs, lists of  
24 personal interests, and other information. Facebook users can also post "status" updates  
25 about their whereabouts and actions, as well as links to videos, photographs, articles, and  
26 other items available elsewhere on the Internet. Facebook users can also post information  
27 about upcoming "events," such as social occasions, by listing the event's time, location,  
28 host, and guest list. A particular user's profile page also includes a "Wall," which is a



1 space where the user and his or her “Friends” can post messages, attachments, and links  
2 that will typically be visible to anyone who can view the user’s profile.

3 38. Facebook has a Photos application, where users can upload an unlimited  
4 number of albums and photos. Another feature of the Photos application is the ability to  
5 “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a  
6 photo or video, he or she receives a notification of the tag and a link to see the photo or  
7 video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by  
8 that user that have not been deleted, as well as all photos uploaded by any user that have  
9 that user tagged in them.

10 39. Facebook users can exchange private messages on Facebook with other  
11 users. These messages, which are similar to e-mail messages, are sent to the recipient’s  
12 “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well  
13 as other information. Facebook users can also post comments on the Facebook profiles  
14 of other users or on their own profiles; such comments are typically associated with a  
15 specific posting or item on the profile.

16 40. Facebook Notes is a blogging feature available to Facebook users, and it  
17 enables users to write and post notes or personal web logs (“blogs”), or to import their  
18 blogs from other services, such as Xanga, LiveJournal, and Blogger.

19 41. The Facebook Gifts feature allows users to send virtual “gifts” to their  
20 friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase,  
21 and a personalized message can be attached to each gift. Facebook users can also send  
22 each other “pokes,” which are free and simply result in a notification to the recipient that  
23 he or she has been “poked” by the sender.

24 42. In addition to the applications described above, Facebook also provides its  
25 users with access to thousands of other applications on the Facebook platform. When a  
26 Facebook user accesses or uses one of these applications, an update about that the user’s  
27 access or use of that application may appear on the user’s profile page.  
28

1           43.     Some Facebook pages are affiliated with groups of users, rather than one  
2 individual user. Membership in the group is monitored and regulated by the  
3 administrator or head of the group, who can invite new members and reject or accept  
4 requests by users to enter. Facebook can identify all users who are currently registered to  
5 a particular group and can identify the administrator and creator of the group. Facebook  
6 also assigns a group identification number to each group. Facebook uses the term  
7 "Group Contact Info" to describe the contact information for the group's creator and  
8 administrator, as well as the current status of the group profile page.

9           44.     Facebook uses the term "Neoprint" to describe an expanded view of a given  
10 user profile. The "Neoprint" for a given user can include the following information from  
11 the user's profile: profile contact information; Mini-Feed information; status updates;  
12 links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists,  
13 including the friends' Facebook user identification numbers; groups and networks of  
14 which the user is a member, including the groups' Facebook group identification  
15 numbers; future and past event postings; rejected "Friend" requests; comments; gifts;  
16 pokes; tags; and information about the user's access and use of Facebook applications.

17           45.     Facebook also retains IP address logs for a given user ID or IP address.  
18 These logs may contain information about the actions taken by the user ID or IP address  
19 on Facebook, including information about the type of action, the date and time of the  
20 action, and the user ID and IP address associated with the action.

21           46.     Social networking providers like Facebook typically retain additional  
22 information about their users' accounts, such as information about the length of service  
23 (including start date), the types of service used, and the means and source of any  
24 payments associated with the service (including any credit card or bank account number).  
25 In some cases, Facebook users may communicate directly with Facebook about issues  
26 relating to their account, such as technical problems, billing inquiries, or complaints from  
27 other users. Social networking providers like Facebook typically retain records about  
28 such communications, including records of contacts between the user and the provider's

1 support services, as well records of any actions taken by the provider or user as a result of  
2 the communications.

3 47. Therefore, the computers of Facebook are likely to contain all the material  
4 just described, including stored electronic communications and information concerning  
5 subscribers and their use of Facebook, such as account access information, transaction  
6 information, and account application.

### 7 **Background Regarding Google's Services**

8 48. In my training and experience, I have learned that Google provides a wide  
9 variety of on-line services, including electronic mail ("e-mail") access and instant  
10 messaging (otherwise known as "chat" messaging), to the general public.

11 49. In addition to e-mail and chat, Google offers subscribers numerous other  
12 services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome  
13 Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google  
14 Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console,  
15 Google Voice, Google+, Google Profile, Location History, Web & Activity, and  
16 YouTube, among others. Thus, a subscriber to a Google account can also store files,  
17 including address books, contact lists, calendar data, photographs and other files, on  
18 servers maintained and/or owned by Google. For example, Google Calendar is a  
19 calendar service that users may utilize to organize their schedule and share events with  
20 others. Google Drive may be used to store data and documents, including spreadsheets,  
21 written documents (such as Word or Word Perfect) and other documents that could be  
22 used to manage a website. Google Photos can be used to create photo albums, store  
23 photographs, and share photographs with others and "You Tube," allows users to view,  
24 store and share videos. Google Search Console records a Google account user's search  
25 queries. And Google Web & Activity records certain browsing history depending on  
26 whether the account holder is logged into their account. Google + is a Google social  
27 networking platform similar to Facebook. This platform provides Google users the  
28 ability to establish accounts through which users can share written news, photographs,

1 videos, and other information with other Facebook users, and sometimes with the general  
2 public.<sup>1</sup> Records and data associated with third party-apps may also be stored on Google;  
3 for example, the app WhatsApp, an instant messaging service owned by Facebook, can  
4 be configured to back up a user's instant messaging to a Google user's account.

5 50. Like many internet service companies, the services Google offers are  
6 constantly changing and evolving.

7 51. Google also offers a suite of cloud computing services that runs on the  
8 same infrastructure that Google uses internally for its end-user products, such as Google  
9 Search and YouTube. Alongside a set of management tools, it provides a series of  
10 modular cloud services including computing, data storage, data analytics and machine  
11 learning to customers.

12 52. Based upon my training and experience, all of these types of information  
13 may be evidence of crimes under investigation. Stored e-mails and chats not only may  
14 contain communications relating to crimes, but also help identify the participants in those  
15 crimes. For example, address books and contact lists may help identify and locate co-  
16 conspirators. Similarly, photographs and videos of co-conspirators may help identify  
17 their true identities, as opposed to supposed identities that they have used in telephone or  
18 e-mail communications. Documents (such as Google sheets used to communicate with  
19 victim computers), may identify the scope of the criminal activity. And calendar data  
20 may reveal the timing and extent of criminal activity. Search and browsing history can  
21 also be extremely useful in identifying those using anonymous online accounts and may  
22 also constitute direct evidence of the crimes under investigation to the extent the  
23 browsing history or search history might include searches and browsing history related to  
24 computer intrusions, point of sale systems, victims, trafficking in stolen data and other  
25 evidence of the crimes under investigation or indications of the true identity of the  
26 account users.

---

27  
28 <sup>1</sup> In October 2018, Google announced it would discontinue the service in approximately August 2019.

**A. Subscriber Records and Account Content**

53. Subscribers obtain an account by registering with Google. When doing so, e-mail providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

54. Google will retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's websites), and other log files that reflect usage of the account. In addition, Google will often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

55. In some cases, Google account users will communicate directly with the provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Google will typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

1        56. Google is also able to provide information that will assist law enforcement  
2 in identifying other accounts associated with the **Target Google Accounts**, namely,  
3 information identifying and relating to other accounts used by the same subscriber. This  
4 information includes any forwarding or fetching accounts<sup>2</sup> relating to the **Target Google**  
5 **Accounts**, all other Google accounts linked to the **Target Google Accounts** because they  
6 were accessed from the same computer (referred to as “cookie overlap”), all other Google  
7 accounts that list the same SMS phone number as the **Target Google Accounts**, all other  
8 Google accounts that list the same recovery e-mail address<sup>3</sup> as do the **Target Google**  
9 **Accounts**, and all other Google accounts that share the same creation IP address as the  
10 **Target Google Accounts**. Information associated with these associated accounts will  
11 assist law enforcement in determining who controls the **Target Google Accounts** and  
12 will also help to identify other e-mail accounts and individuals relevant to the  
13 investigation.

#### 14                    **Google Location History and Location Reporting**

15        57. According to Google’s website, “Location Reporting” allows Google to  
16 periodically store and use a device’s most recent location data in connection with the  
17 Google Account connected to the device. “Location History” allows Google to store a  
18 history of location data from all devices where a user is logged into their Google Account  
19 and have enabled Location Reporting. According to Google “when you turn on Location  
20 Reporting for a device like your iPhone or iPad, it lets Google periodically store and use  
21 that device’s most recent location data in connection with your Google Account.” How  
22 often Location Reporting updates location data is not fixed. Frequency is determined by  
23 factors such as how much battery life the device has, if the device is moving, or how fast  
24

25        <sup>2</sup> A forwarding or fetching account related to the **Target Google Accounts** would be a separate e-mail account that  
26 can be setup by the user to receive copies of all of the e-mail sent to the **Target Google Accounts**.

27        <sup>3</sup> The recovery e-mail address is an additional e-mail address supplied by the user that is used by Google to confirm  
28 your username after you create an e-mail account, help you if you are having trouble signing into your Google  
account or have forgotten your password, or alert you to any unusual activity involving user’s Google e-mail  
address.



1 the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and  
2 cellular network towers to determine an account holder's location.

3 58. Based on the above, I know that if a user of the **Target Google Accounts**  
4 utilizes a mobile device to access the respective account identified in Attachment A3 and  
5 has not disabled location services on his or her device/s or through the Google account  
6 settings, Google may have detailed records of the locations at which the account holders  
7 utilized the mobile device/s. This type of evidence may further assist in identifying the  
8 account holders, and lead to the discovery of other evidence of the crimes under  
9 investigation.

10 59. I know that Google's Android service collects and stores identifying  
11 information about an Android smart phone used to access the Google account, including  
12 the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber  
13 Identity (IMSI), telephone number and mobile carrier code. I know that Google's  
14 Location History service periodically queries the physical location of a device that is  
15 currently accessing a Google account through the device's GPS, nearby Wi-Fi network  
16 IDs and cellular tower information and records a history of device movements in  
17 Google's servers. Because the criminal actors behind this malware scheme have made a  
18 concerted effort to disguise their real location, I am requesting Google to provide  
19 information from the Android service and Location History service from the **Target**  
20 **Google Accounts** in order to more accurately identify the location and phone number of  
21 the person responsible for the **Target Google Accounts**.

22 **Information To Be Searched And Things To Be Seized**

23 60. Pursuant to Title 18, United States Code, Section 2703(g), this application  
24 and affidavit for search warrants seeks authorization to permit T-Mobile Wireless,  
25 Facebook, Inc., and Google, Inc., and its agents and employees, to assist agents in the  
26 execution of this warrant. Once issued, the search warrants will be presented to T-Mobile  
27 Wireless, Facebook, Inc., and Google, Inc. with direction that each entity identify the  
28 account described in Attachments A1-3 to this affidavit, respectively, as well as other



1 subscriber and log records associated with each of the accounts, as set forth in Section I  
2 of Attachments B1-3 to this affidavit.

3 61. The search warrant will direct T-Mobile Wireless, Facebook, Inc., and  
4 Google, Inc. to create an exact copy of the specified account and records, including an  
5 exact copy of the contents of the hard disk drive or drives installed on the server  
6 associated with the **Target Accounts**, or the original drives.

7 62. I, and/or other law enforcement personnel will thereafter review the copy of  
8 the electronically stored data, and identify from among that content those items that come  
9 within the items identified in Section II to Attachment B, for seizure.

10 63. Analyzing the data contained in the forensic image may require special  
11 technical skills, equipment, and software. It could also be very time-consuming.  
12 Searching by keywords, for example, can yield thousands of “hits,” each of which must  
13 then be reviewed in context by the examiner to determine whether the data is within the  
14 scope of the warrant. Merely finding a relevant “hit” does not end the review process.  
15 Keywords used originally need to be modified continuously, based on interim results.  
16 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,  
17 search text, and many common e-mail, database and spreadsheet applications do not store  
18 data as searchable text. The data may be saved, instead, in proprietary non-text format.  
19 And, as the volume of storage allotted by service providers increases, the time it takes to  
20 properly analyze recovered data increases, as well. Consistent with the foregoing,  
21 searching the recovered data for the information subject to seizure pursuant to this  
22 warrant may require a range of data analysis techniques and may take weeks or even  
23 months. All forensic analysis of the data will employ only those search protocols and  
24 methodologies reasonably designed to identify and seize the items identified in Section II  
25 of Attachment B to the warrant.

26 **V. REQUEST FOR DELAYING NOTICE**

27 64. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of  
28 Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to

1 delay notice until 30 days after the collection authorized by the warrant has been  
2 completed. This delay is justified because there is reasonable cause to believe that  
3 providing immediate notification of the warrant may have an adverse result, as defined in  
4 18 U.S.C. § 2705. Based upon my knowledge, training, and experience, it is my belief  
5 that providing immediate notice to subscriber or user of the **Target Cell Phone,**  
6 **Facebook, and Google Accounts** may result in premature notification to Kamden, or the  
7 subscriber, of the existence of the authorization for telephone location tracking would  
8 alert them to the ongoing investigation, and this disclosure would jeopardize the  
9 continuation and efficacy of the investigation. Furthermore, premature notification to  
10 Kamden or the subscriber of the existence of the authorization for telephone location  
11 tracking prior to completion of the investigation would provide Kamden or the subscriber  
12 the opportunity to destroy evidence and flee the jurisdiction. *See* 18 U.S.C.  
13 § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the  
14 warrant, the proposed search warrant does not authorize the seizure of any tangible  
15 property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant  
16 authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. §  
17 2510) or any stored wire or electronic information, there is reasonable necessity for the  
18 seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

## 19 VI. REQUEST FOR SEALING

20 65. I further request this Court issue an order sealing, until further order of the  
21 Court, all papers submitted in support of the requested search warrant, including the  
22 application, this affidavit, the attachments, and the requested search warrant. I believe  
23 sealing these documents is necessary because the information to be seized is relevant to  
24 an ongoing investigation, and any disclosure of the information at this time may cause  
25 Kamden, Djoko, Fanyo-Patcho, or others associated with **Target Cell Phone, Facebook,**  
26 **and Google Accounts**, to flee from prosecution, cause destruction of or tampering with  
27 evidence, or otherwise seriously jeopardize this investigation. Premature disclosure of  
28

1 the contents of the application, this affidavit, the attachments, and the requested search  
2 warrant may adversely affect the integrity of the investigation.

3 **VII. CONCLUSION**

4 66. Based on the foregoing, I request that the Court issue the proposed search  
5 warrants, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I  
6 further request that the Court authorize execution of the warrant at any time of day or  
7 night, owing to the potential need to locate the **Target Cell Phone, Facebook, and**  
8 **Google Accounts** outside of daytime hours. Pursuant to 18 U.S.C. § 2703(g), the  
9 presence of a law enforcement officer is not required for the service or execution of this  
10 warrant. Accordingly, by this Affidavit and warrant I seek authority for the government  
11 to search all of the items specified in Section I of Attachment B1-3 (attached hereto and  
12 incorporated by reference herein) to the warrant, and specifically to seize all of the data,  
13 documents and records that are identified in Section II to that same Attachment.

14 67. I further request that the Court direct Provider to disclose to the government  
15 any information described in Attachment B that is within the possession, custody, or  
16 control of Provider. I also request that the Court direct Provider to furnish the  
17 government all information, facilities, and technical assistance necessary to accomplish  
18 the collection of the information described in Attachment B unobtrusively and with a  
19 minimum of interference with Provider's services, including by initiating a signal to  
20 determine the location of the **Target Cell Phone, Facebook, and Google Accounts** on  
21 Provider's network or with such other reference points as may be reasonably available,  
22 and at such intervals and times directed by the government.

23 //

24 //

25 //

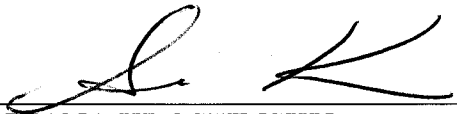
26 //

27

28

1 I declare under the penalty of perjury that the statements above are true and correct  
2 to the best of my knowledge and belief.

3 DATED this 21st day of December 2018.

4  
5   
6 ARIANA KROSHINSKY  
7 Special Agent  
8 Federal Bureau of Investigations  
9

10 SUBSCRIBED AND SWORN before me this on this 21st day of December, 2018.

11  
12   
13 MARY ALICE THEILER  
14 United States Magistrate Judge  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**ATTACHMENT A-1**

**Target Cell Phone**

1. This warrant applies to information associated with the cellular telephone assigned call number **206-407-4936**, with an International Mobile Subscriber Identifier (“IMSI”) number or Electronic Serial Number (“ESN”) 353322/09/047605/3 (hereinafter “**Target Cell Phone**”), that is stored at the premises owned, maintained, controlled, and/or operated T-Mobile Wireless, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, WA 98006.

**ATTACHMENT B-1**

**T-Mobile - Particular Things to be Seized**

**A. The following information about the customers or subscribers of the Account(s):**

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account numbers) and billing records.

**B. All records and other information (not including the contents of communications) relating to the Account, including:**

9. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

10. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers), and;

11. All information about the location of the Target Cell Phone described in Attachment A1 from October 20, 2018 through November 3, 2018, during all times of day and night, and the status of the device and the account associated with the device (i.e., whether the device is active or operational and whether the account is in good standing, canceled, suspended, etc.). "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A1.

12. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of (wireless provider) (hereinafter "Provider"), Provider is required to disclose the Location Information to the government. In addition, Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Provider for reasonable expenses incurred in furnishing such facilities or assistance.

13. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds it reasonable necessity for the seizure of the Location Information. See 18 U.S.C § 3103a(b)(2).



**ATTACHMENT A-2**

**Target Accounts Facebook, Inc.**

1. This warrant applies to information associated with Facebook user IDs:

- a. 1279801734;
- b. 100023633720499; and
- c. 100002532176517

that are stored at the premises owned, maintained, controlled, or operated by Facebook, Inc. located at 1601 Willow Road, Menlo Park, California.

## **ATTACHMENT B -2**

### **Facebook - Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information for the account described in Attachment A-2, is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A-2:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

- of;
- (i) All information about the Facebook pages that the account is or was a “fan”
  - (j) All past and present lists of friends created by the account;
  - (k) All records of Facebook searches performed by the account;
  - (l) All information about the user’s access and use of Facebook Marketplace;
  - (m) The types of service utilized by the user;
  - (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
  - (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
  - (p) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that relates to the ongoing investigation of violations of 18 U.S.C. § § 241 and 249 (Conspiracy to Violate Civil Rights and Hate Crimes); and 18 U.S.C. § 2261A (Cyberstalking) involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, including, for each user ID identified on Attachment A-2, information pertaining to the following matters:

- (a) Any content including e-mails, messages, texts, photographs, visual images, documents, spreadsheets, address lists, contact lists or communications of any type which could be used to identify the user and or their location;

(b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

(c) All subscriber records associated with the specified accounts, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number;

(d) Any and all other log records, including IP address captures, associated with the specified accounts; and

(e) Any records of communications between Facebook and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

**ATTACHMENT A-3**

**Target Accounts Google, Inc.**

1. This warrant applies to information associated with Google user identification numbers and Google + user id #'s:

- a. 117906598794476810352; and
- b. 114036295919816718188

that are stored at the premises owned, maintained, controlled, or operated by Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B-3**

**Google - Particular Things to be Seized**

**Section I - Information to be disclosed by Google, for search:**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Google, including any e-mails, records, files, logs, backup data from third party apps such as WhatsApp, or information that has been deleted but is still available to Google or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.**

## **Section II - Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 241 and 249 (conspiracy to violate civil rights or hate crimes); 18 U.S.C. §§ 2261A (Cyberstalking), involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

- a. The cyberstalking and harassment of U.M.;
- b. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- c. Any address lists or buddy/contact lists associated with the specified account;
- d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;
- e. Any and all other log records, including IP address captures, associated with the specified account;
- f. Any records of communications between Google, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.



## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 Target Cell Phone, more particularly described in  
 Attachment A1

Case No.

MJ18-584 (1)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
 of the following person or property located in the Western District of Washington  
 (identify the person or describe the property to be searched and give its location):

Target Cell Phone, cellular telephone assigned call number 206-407-4936 of T-Mobile Wireless, more particularly described  
 in Attachment A1, attached hereto and incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
 described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B1 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan 4, 2019 (not to exceed 14 days)  
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
 person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
 property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
 as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge  
 (United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
 § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
 property, will be searched or seized (check the appropriate box)

☐ for        days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019

Date and time issued: Dec 21, 2018  
11:30 AM

Mary Alice Theiler  
 Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A-1**

**Target Cell Phone**

1. This warrant applies to information associated with the cellular telephone assigned call number **206-407-4936**, with an International Mobile Subscriber Identifier (“IMSI”) number or Electronic Serial Number (“ESN”) 353322/09/047605/3 (hereinafter “**Target Cell Phone**”), that is stored at the premises owned, maintained, controlled, and/or operated T-Mobile Wireless, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, WA 98006.

**ATTACHMENT B-1**

**T-Mobile - Particular Things to be Seized**

**A. The following information about the customers or subscribers of the Account(s):**

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account numbers) and billing records.

**B. All records and other information (not including the contents of communications) relating to the Account, including:**

9. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

10. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers), and;

11. All information about the location of the Target Cell Phone described in Attachment A1 from October 20, 2018 through November 3, 2018, during all times of day and night, and the status of the device and the account associated with the device (i.e., whether the device is active or operational and whether the account is in good standing, canceled, suspended, etc.). "Information about the location of the Target Cell Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which "cell towers" (i.e., antenna towers covering specific geographic areas) and "sectors" (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A1.

12. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of (wireless provider) (hereinafter "Provider"), Provider is required to disclose the Location Information to the government. In addition, Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Provider for reasonable expenses incurred in furnishing such facilities or assistance.

13. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds it reasonable necessity for the seizure of the Location Information. See 18 U.S.C § 3103a(b)(2).

Magistrate Judge Mary Alice Theiler

DEC 21 2018

CLERK OF DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF:

NO. MJ18-584 (1)

T-Mobile Wireless Telephone Number  
206-407-4936

MOTION TO SEAL SEARCH  
WARRANT AND RELATED  
MATERIALS

(Filed Under Seal)

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, and Bruce F. Miyake, Assistant United States Attorney, respectfully requests that this Search Warrant, Application for Search Warrant, and related documents in this matter, including this Motion and its attendant Order, be sealed as set forth below, to protect the ongoing criminal investigation. The United States of America further respectfully requests that notwithstanding the requested sealing order, the Government retain the authority to produce the materials subject to this Court's sealing order as part of its discovery obligations in a criminal case.

Federal courts are empowered to seal documents in appropriate circumstances. *Cf.* Fed. R. Crim. P. 6(e)(4) (sealing of indictments). It is well-settled that federal courts have inherent authority to control papers filed with the court, *United States v. Shryock*, 342 F.3d 948, 983 (9th Cir. 2003), including the power to seal affidavits filed with search

1 warrants in appropriate circumstances. In *Times Mirror Company v. United States*, 873  
2 F.2d 1210 (9th Cir. 1989), the Court recognized that “information disclosed to the  
3 magistrate in support of the warrant request is entitled to the same confidentiality  
4 accorded other aspects of the criminal investigation.” *Id.* at 1214. This inherent power  
5 may appropriately be exercised when disclosure of the affidavit would disclose facts that  
6 would interfere with an ongoing criminal investigation. *United States v. Napier*, 436  
7 F.3d 1133, 1136 (9th Cir. 2006) (noting that a sealed search warrant protects the  
8 “government’s interest in maintaining [the] integrity of ongoing criminal investigations  
9 and ensuring the safety of the informant”).

10 In support of this request, the government states that the public disclosure of any  
11 of these materials at this juncture could jeopardize the government’s ongoing  
12 investigation in this case because the government believes the investigation will  
13 ultimately lead to other individuals involved in illegal activity, including cyber stalking.  
14 Thus public disclosure of these materials could cause the targets of the investigation to  
15 destroy evidence or flee prosecution.

16 Therefore, the United States of America respectfully requests that the documents  
17 in this case be sealed until sealed until the earliest of the following: (a) two weeks  
18 following the unsealing of any charging document in a matter for which the warrants  
19 were issued; (b) two weeks following the closure of the investigation for which the  
20 warrants were issued; or (c) ninety days following issuance of the warrant, unless the  
21 Court, upon motion of the government for good cause, orders an extension of the Order.

22 DATED this 21st day of December, 2018.

23  
24 Respectfully submitted,

25 ANNETTE L. HAYES  
26 United States Attorney

27 s/ Bruce F. Miyake

28 BRUCE F. MIYAKE

Assistant United States Attorney



Magistrate Judge Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF:

NO.

**MJ18-584 (1)**

T-Mobile Wireless Telephone Number  
206-407-4936

ORDER SEALING SEARCH WARRANT  
AND RELATED MATERIALS

**(Filed Under Seal)**

Based upon the motion of the United States, and the representations made therein,  
and good cause having been show:

IT IS HEREBY ORDERED that the search warrant, search warrant return,  
application and affidavits in support of the same, and all attachments in this matter, along  
with this motion and order, shall be sealed and shall remain sealed until the earliest of  
the following: (a) two weeks following the unsealing of any charging document in a  
matter for which the warrants were issued; (b) two weeks following the closure of the  
investigation for which the warrants were issued; or (c) ninety days following issuance of  
the warrant, unless the Court, upon motion of the government for good cause, orders an  
extension of this Order. Nothing in this Order is intended to create or supersede any  
other applicable obligation under law.

IT IS FURTHER ORDERED, that on or before the earliest of the dates specified  
above, the government shall file a motion in which it either (1) provides good cause for a  
further order of this Court permitting these documents to remain under seal for an


ORDER SEALING SEARCH WARRANT  
AND RELATED MATERIALS - 1  
USAO #2018R01525

UNITED STATES ATTORNEY  
700 STEWART STREET, SUITE 5220  
SEATTLE, WASHINGTON 98101  
(206) 553-7970

1 additional period of time, or (2) requests an order of this Court to unseal this warrant and  
2 all related documents, including the motion and order to seal the same. In the event the  
3 government fails to file the motion required by this Order on or before the earliest of the  
4 three triggering events, and the Court has not otherwise extended the sealing period  
5 following a showing of good cause by the government, the Clerk of Court shall unseal  
6 this warrant and all related documents without further order of the Court.

7 IT IS SO ORDERED.

8 DATED this 21st day of December, 2018.

9  
10   
11 MARY ALICE THEILER  
12 United States Magistrate Judge

13 Presented by:

14 s/ Bruce F. Miyake  
15 BRUCE F. MIYAKE  
16 Assistant United States Attorney  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## UNITED STATES DISTRICT COURT

for the  
Western District of WashingtonIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Target Facebook Accounts, more particularly described  
in Attachment A2

Case No.

MJ18-584 (2)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):Target Facebook, Inc. Accounts, user IDs 1279801734, 100023633720499, and 100002532176517, more particularly  
described in Attachment A2, attached hereto and incorporated herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B2 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan. 4, 2019 (not to exceed 14 days)  
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for        days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019Date and time issued: 12/21/2018 at 11:30 AM  
Judge's signatureCity and state: Seattle, WashingtonMary Alice Theiler, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A-2**

**Target Accounts Facebook, Inc.**

1. This warrant applies to information associated with Facebook user IDs:

- a. 1279801734;
- b. 100023633720499; and
- c. 100002532176517

that are stored at the premises owned, maintained, controlled, or operated by Facebook, Inc. located at 1601 Willow Road, Menlo Park, California.

## **ATTACHMENT B -2**

### **Facebook - Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information for the account described in Attachment A-2, is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A-2:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

- of;
- (i) All information about the Facebook pages that the account is or was a “fan”
  - (j) All past and present lists of friends created by the account;
  - (k) All records of Facebook searches performed by the account;
  - (l) All information about the user’s access and use of Facebook Marketplace;
  - (m) The types of service utilized by the user;
  - (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
  - (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
  - (p) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that relates to the ongoing investigation of violations of 18 U.S.C. § § 241 and 249 (Conspiracy to Violate Civil Rights and Hate Crimes); and 18 U.S.C. § 2261A (Cyberstalking) involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, including, for each user ID identified on Attachment A-2, information pertaining to the following matters:

- (a) Any content including e-mails, messages, texts, photographs, visual images, documents, spreadsheets, address lists, contact lists or communications of any type which could be used to identify the user and or their location;



(b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

(c) All subscriber records associated with the specified accounts, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number;

(d) Any and all other log records, including IP address captures, associated with the specified accounts; and

(e) Any records of communications between Facebook and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Magistrate Judge Mary Alice Theiler

DEC 21 2018

CLERK OF DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF  
CERTAIN FACEBOOK, INC. USER  
ACCOUNTS:

1279801734, 100023633720499, and  
100002532176517

NO.

**MJ18-584 (2)**

MOTION TO SEAL SEARCH  
WARRANT MATERIALS AND FOR  
NONDISCLOSURE ORDER

**(Filed Under Seal)**

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, and Bruce F. Miyake, Assistant United States Attorney for said District, moves this Court for an Order sealing the Search Warrant, Application for Search Warrant, and Affidavit of Special Agent Ariana Kroshinsky, as well as this Motion and attendant Order. The government further requests that this Order prohibit Facebook, Inc. from disclosing the existence of the Search Warrant to the account holders, or any other persons. Absent such an Order, it is the policy of Facebook, Inc. to notify users of legal process, which would jeopardize the ongoing federal investigation.

Specifically, providing the targets with notice of the search warrant would inform the target about the government's interest in specific Facebook, Inc. accounts not previously subject to a search warrant, giving the targets additional information about the

1 direction of the investigation and an opportunity to identify and potentially tamper with  
2 evidence and witnesses.

3 Federal courts are empowered to seal documents in appropriate circumstances.  
4 Cf. Fed. R. Crim. P. 6(e)(4) (sealing of indictments). It is well-settled that federal courts  
5 have inherent authority to control papers filed with the court, *United States v. Shryock*,  
6 342 F.3d 948, 983 (9th Cir. 2003), including the power to seal affidavits filed with search  
7 warrants in appropriate circumstances. In *Times Mirror Company v. United States*,  
8 873 F.2d 1210 (9th Cir. 1989), the Court recognized that “information disclosed to the  
9 magistrate in support of the warrant request is entitled to the same confidentiality  
10 accorded other aspects of the criminal investigation.” *Id.* at 1214. This inherent power  
11 may appropriately be exercised when disclosure of the affidavit would disclose facts that  
12 would interfere with an ongoing criminal investigation. *United States v. Napier*,  
13 436 F.3d 1133, 1136 (9th Cir. 2006) (noting that a sealed search warrant protects the  
14 “government’s interest in maintaining [the] integrity of ongoing criminal investigations  
15 and ensuring the safety of the informant”).

16 In support of this request, the government submits that the Search Warrant  
17 documents detail of an ongoing investigation into the suspected criminal activities of the  
18 Facebook, Inc. account users and others. The Government expects that the investigation  
19 will continue after the execution of the search warrant, and may involve additional  
20 searches, interviews, and subpoenas. Premature revelation of the details of the  
21 investigation, including which Facebook, Inc. accounts, Facebook, Inc. messages, and  
22 witnesses relate to the investigation, may impede the investigation by encouraging the  
23 suspects to destroy evidence or influence witnesses. Since there is no reason to reveal the  
24 details of the investigation until such time as a court determines that it is necessary to  
25 permit an indicted defendant to attack the validity of the search, the Government moves  
26 for an Order sealing the warrant and related materials.

27 Therefore, the United States of America respectfully requests that the documents  
28 in this case be sealed until the earliest of the following: (a) two weeks following the

1 unsealing of any charging document in a matter for which the warrant was issued; (b) two  
2 weeks following the closure of the investigation for which the warrant was issued; or (c)  
3 sixteen months following issuance of the warrant, unless the Court, upon motion of the  
4 government for good cause, orders an extension of the Order.

5 For the same reasons, the government further requests, pursuant to the preclusion  
6 of notice provisions of Title 18, United States Code, Section 2705(b), that Facebook, Inc.  
7 be precluded from notifying any persons (including the subscribers or customers to which  
8 the materials relate) of the existence of this warrant for a period of one year from the date  
9 of the Order, except that Facebook, Inc. may disclose the warrant to an attorney for  
10 Facebook, Inc. for the purpose of receiving legal advice.

11 DATED this 21st day of December, 2018.

12  
13 Respectfully submitted,

14 ANNETTE L. HAYES  
15 United States Attorney

16 s/ Bruce F. Miyake  
17 BRUCE F. MIYAKE  
18 Assistant United States Attorney  
19 700 Stewart Street, Suite 5220  
20 Seattle, WA 98101-1271  
21 Telephone: (206) 553-2077  
22 E-mail: Bruce.Miyake@usdoj.gov  
23  
24  
25  
26  
27  
28

Magistrate Judge Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF  
FACEBOOK, INC. USER ACCOUNTS:

1279801734, 100023633720499, and  
100002532176517

NO.

*MJ18-584 (2)*

ORDER SEALING SEARCH WARRANT  
AND RELATED MATERIALS AND  
PROHIBITING DISCLOSURE

(Filed Under Seal)

The government has moved to seal the search warrant and related materials in this case. Good cause having been shown, now, therefore,


IT IS HEREBY ORDERED that the Search Warrant, search warrant return, Application, and Affidavit for search warrant, the government's motion, and this Order be sealed until the earlier of the following: (a) two weeks following the unsealing of any charging document in a matter for which the warrant was issued, (b) two weeks following the closure of the investigation for which the warrant was issued, or (c) sixteen months following the date of this Order, unless the Court, upon motion of the government for good cause, orders an extension of this Order. Nothing in this Order is intended to create or supersede any other application obligation under law.

IT IS FURTHER ORDERED, that on or before the earliest of the dates specified above, the government shall file a motion in which it either (1) provides good cause for a further order of this Court permitting these documents to remain under seal for an

1 additional period of time, or (2) requests an order of this Court to unseal this warrant and  
2 all related documents, including the motion and order to seal the same. In the event the  
3 government fails to file the motion required by this Order on or before the earliest of the  
4 three triggering events, and the Court has not otherwise extended the sealing period  
5 following a showing of good cause by the government, the Clerk of Court shall unseal  
6 this warrant and all related documents without further order of the Court.

7 IT IS HEREBY FURTHER ORDERED that, pursuant to the preclusion of notice  
8 provisions of Title 18, United States Code, Section 2705(b), Facebook, Inc. shall be  
9 precluded from notifying any persons (including the subscribers or customers to which  
10 the materials relate) of the existence of this warrant until one year from the date of this  
11 Order, except that Facebook, Inc. may disclose the warrant to an attorney for Facebook,  
12 Inc. for the purpose of receiving legal advice.

13 DATED this 21st day of December, 2018.

14  
15   
16 MARY ALICE THEILER  
17 United States Magistrate Judge

18 Presented by:

19 s/ Bruce F. Miyake

20 BRUCE F. MIYAKE

21 Assistant United States Attorney  
22  
23  
24  
25  
26  
27  
28

## UNITED STATES DISTRICT COURT

for the  
Western District of WashingtonIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Target Google Accounts, more particularly described in  
Attachment A3

Case No.

MJ18-584 (3)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):Target Google, Inc. Accounts, user IDs 117906598794476810352 and 114036295919816718188, more particularly  
described in Attachment A3, attached hereto and incorporated herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B3 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan. 4, 2019 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019Date and time issued: 12/21/2018 at 11:30 AM  
Judge's signatureCity and state: Seattle, WashingtonMary Alice Theiler, United States Magistrate Judge

Printed name and title



AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A-3**

**Target Accounts Google, Inc.**

1. This warrant applies to information associated with Google user identification numbers and Google + user id #'s:

- a. 117906598794476810352; and
- b. 114036295919816718188

that are stored at the premises owned, maintained, controlled, or operated by Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

**ATTACHMENT B-3**

**Google - Particular Things to be Seized**

**Section I - Information to be disclosed by Google, for search:**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Google, including any e-mails, records, files, logs, backup data from third party apps such as WhatsApp, or information that has been deleted but is still available to Google or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.**

## **Section II - Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 241 and 249 (conspiracy to violate civil rights or hate crimes); 18 U.S.C. §§ 2261A (Cyberstalking), involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

- a. The cyberstalking and harassment of U.M.;
- b. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- c. Any address lists or buddy/contact lists associated with the specified account;
- d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;
- e. Any and all other log records, including IP address captures, associated with the specified account;
- f. Any records of communications between Google, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Magistrate Judge Mary Alice Theiler

DEC 21 2018

AT SEATTLE  
CLERK OF DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF  
CERTAIN GOOGLE, INC. USER  
ACCOUNTS:

117906598794476810352 and  
114036295919816718188

NO. **MJ18-584 (3)**

MOTION TO SEAL SEARCH  
WARRANT MATERIALS AND FOR  
NONDISCLOSURE ORDER

**(Filed Under Seal)**

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, and Bruce F. Miyake, Assistant United States Attorney for said District, moves this Court for an Order sealing the Search Warrant, Application for Search Warrant, and Affidavit of Special Agent Ariana Kroshinsky, as well as this Motion and attendant Order. The government further requests that this Order prohibit Google, Inc. from disclosing the existence of the Search Warrant to the account holders, or any other persons. Absent such an Order, it is the policy of Google, Inc. to notify users of legal process, which would jeopardize the ongoing federal investigation.

Specifically, providing the targets with notice of the search warrant would inform the target about the government's interest in specific Google, Inc. accounts not previously subject to a search warrant, giving the targets additional information about the direction

1 of the investigation and an opportunity to identify and potentially tamper with evidence  
2 and witnesses.

3 Federal courts are empowered to seal documents in appropriate circumstances.  
4 Cf. Fed. R. Crim. P. 6(e)(4) (sealing of indictments). It is well-settled that federal courts  
5 have inherent authority to control papers filed with the court, *United States v. Shryock*,  
6 342 F.3d 948, 983 (9th Cir. 2003), including the power to seal affidavits filed with search  
7 warrants in appropriate circumstances. In *Times Mirror Company v. United States*,  
8 873 F.2d 1210 (9th Cir. 1989), the Court recognized that “information disclosed to the  
9 magistrate in support of the warrant request is entitled to the same confidentiality  
10 accorded other aspects of the criminal investigation.” *Id.* at 1214. This inherent power  
11 may appropriately be exercised when disclosure of the affidavit would disclose facts that  
12 would interfere with an ongoing criminal investigation. *United States v. Napier*,  
13 436 F.3d 1133, 1136 (9th Cir. 2006) (noting that a sealed search warrant protects the  
14 “government’s interest in maintaining [the] integrity of ongoing criminal investigations  
15 and ensuring the safety of the informant”).

16 In support of this request, the government submits that the Search Warrant  
17 documents detail of an ongoing investigation into the suspected criminal activities of the  
18 Google, Inc. account users and others. The Government expects that the investigation  
19 will continue after the execution of the search warrant, and may involve additional  
20 searches, interviews, and subpoenas. Premature revelation of the details of the  
21 investigation, including which Google, Inc. accounts, Google, Inc. messages, and  
22 witnesses relate to the investigation, may impede the investigation by encouraging the  
23 suspects to destroy evidence or influence witnesses. Since there is no reason to reveal the  
24 details of the investigation until such time as a court determines that it is necessary to  
25 permit an indicted defendant to attack the validity of the search, the Government moves  
26 for an Order sealing the warrant and related materials.

27 Therefore, the United States of America respectfully requests that the documents  
28 in this case be sealed until the earliest of the following: (a) two weeks following the

1 unsealing of any charging document in a matter for which the warrant was issued; (b) two  
2 weeks following the closure of the investigation for which the warrant was issued; or (c)  
3 sixteen months following issuance of the warrant, unless the Court, upon motion of the  
4 government for good cause, orders an extension of the Order.

5 For the same reasons, the government further requests, pursuant to the preclusion  
6 of notice provisions of Title 18, United States Code, Section 2705(b), that Google, Inc. be  
7 precluded from notifying any persons (including the subscribers or customers to which  
8 the materials relate) of the existence of this warrant for a period of one year from the date  
9 of the Order, except that Google, Inc. may disclose the warrant to an attorney for Google,  
10 Inc. for the purpose of receiving legal advice.

11 DATED this 21st day of December, 2018.

12  
13 Respectfully submitted,

14 ANNETTE L. HAYES  
15 United States Attorney

16 s/ Bruce F. Miyake  
17 BRUCE F. MIYAKE  
18 Assistant United States Attorney  
19 700 Stewart Street, Suite 5220  
20 Seattle, WA 98101-1271  
21 Telephone: (206) 553-2077  
22 E-mail: Bruce.Miyake@usdoj.gov  
23  
24  
25  
26  
27  
28

Magistrate Judge Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE SEARCH OF  
GOOGLE, INC. USER ACCOUNTS:

117906598794476810352 and  
114036295919816718188

NO.

MJ18-584 (3)

ORDER SEALING SEARCH WARRANT  
AND RELATED MATERIALS AND  
PROHIBITING DISCLOSURE

(Filed Under Seal)

The government has moved to seal the search warrant and related materials in this case. Good cause having been shown, now, therefore,

IT IS HEREBY ORDERED that the Search Warrant, search warrant return, Application, and Affidavit for search warrant, the government's motion, and this Order be sealed until the earlier of the following: (a) two weeks following the unsealing of any charging document in a matter for which the warrant was issued, (b) two weeks following the closure of the investigation for which the warrant was issued, or (c) sixteen months following the date of this Order, unless the Court, upon motion of the government for good cause, orders an extension of this Order. Nothing in this Order is intended to create or supersede any other application obligation under law.


IT IS FURTHER ORDERED, that on or before the earliest of the dates specified above, the government shall file a motion in which it either (1) provides good cause for a further order of this Court permitting these documents to remain under seal for an



1 additional period of time, or (2) requests an order of this Court to unseal this warrant and  
2 all related documents, including the motion and order to seal the same. In the event the  
3 government fails to file the motion required by this Order on or before the earliest of the  
4 three triggering events, and the Court has not otherwise extended the sealing period  
5 following a showing of good cause by the government, the Clerk of Court shall unseal  
6 this warrant and all related documents without further order of the Court.

7 IT IS HEREBY FURTHER ORDERED that, pursuant to the preclusion of notice  
8 provisions of Title 18, United States Code, Section 2705(b), Google, Inc. shall be  
9 precluded from notifying any persons (including the subscribers or customers to which  
10 the materials relate) of the existence of this warrant until one year from the date of this  
11 Order, except that Google, Inc. may disclose the warrant to an attorney for Google, Inc.  
12 for the purpose of receiving legal advice.

13 DATED this 21st day of December, 2018.

14  
15   
16 MARY ALICE THEILER  
17 United States Magistrate Judge

18 Presented by:

19 s/ Bruce F. Miyake  
20 BRUCE F. MIYAKE  
21 Assistant United States Attorney  
22  
23  
24  
25  
26  
27  
28

AO 93 (Rev. 11/13) Search and Seizure Warrant

## UNITED STATES DISTRICT COURT

for the

Western District of Washington

<u>      </u> FILED	<u>      </u> ENTERED
<u>      </u> LODGED	<u>      </u> RECEIVED

FEB 01 2019 GT

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
Target Cell Phone, more particularly described in )  
Attachment A1 )  
)

Case No.

MJ18-584 (1)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):

Target Cell Phone, cellular telephone assigned call number 206-407-4936 of T-Mobile Wireless, more particularly described in Attachment A1, attached hereto and incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B1 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan 4, 2019 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge  
(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for        days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019

Date and time issued:

Dec 21, 2018  
11:30 AM

Mary Alice Theiler  
Judge's signature

City and state:

Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

Case No.:

MJ18-584(1)

Date and time warrant executed:

1/2/19, 4:08 PM

Copy of warrant and inventory left with:

T-mobile Metro PCS

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

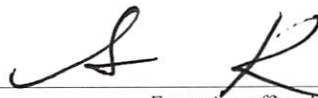
Digital data including call log and GPS location  
of target cell phone 206-407-4936

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

1/31/19

Executing officer's signature

SA Ariana Kroshinsky

Printed name and title

**ATTACHMENT A-1**

**Target Cell Phone**

1. This warrant applies to information associated with the cellular telephone assigned call number **206-407-4936**, with an International Mobile Subscriber Identifier (“IMSI”) number or Electronic Serial Number (“ESN”) 353322/09/047605/3 (hereinafter “**Target Cell Phone**”), that is stored at the premises owned, maintained, controlled, and/or operated T-Mobile Wireless, a wireless telephone service provider headquartered at 3625 132nd Ave SE, Bellevue, WA 98006.

**ATTACHMENT B-1**

**T-Mobile - Particular Things to be Seized**

**A. The following information about the customers or subscribers of the**

**Account(s):**

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account numbers) and billing records.

**B. All records and other information (not including the contents of communications) relating to the Account, including:**

9. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

10. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers), and;

11. All information about the location of the Target Cell Phone described in Attachment A1 from October 20, 2018 through November 3, 2018, during all times of day and night, and the status of the device and the account associated with the device (i.e., whether the device is active or operational and whether the account is in good standing, canceled, suspended, etc.). “Information about the location of the Target Cell Phone” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from the cellular telephone described in Attachment A1.

12. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of (wireless provider) (hereinafter “Provider”), Provider is required to disclose the Location Information to the government. In addition, Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with Provider’s services, including by initiating a signal to determine the location of the Target Cell Phone on Provider’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate Provider for reasonable expenses incurred in furnishing such facilities or assistance.

13. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds it reasonable necessity for the seizure of the Location Information. See 18 U.S.C § 3103a(b)(2).



AO 93 (Rev. 11/13) Search and Seizure Warrant

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED

LODGED

ENTERED

RECEIVED

FEB 01 2019 GT

BY AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTYIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Target Facebook Accounts, more particularly described  
in Attachment A2

Case No.

MJ18-584 (2)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):Target Facebook, Inc. Accounts, user IDs 1279801734, 100023633720499, and 100002532176517, more particularly  
described in Attachment A2, attached hereto and incorporated herein.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B2 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan. 4, 2019 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge  
(United States Magistrate Judge)☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for \_\_\_\_\_ days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019.Date and time issued: 12/21/2018 at 11:30 AM  
Judge's signatureCity and state: Seattle, WashingtonMary Alice Theiler, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

Case No.:

MJ18-584(2)

Date and time warrant executed:

1/2/19, 3:24 PM

Copy of warrant and inventory left with:

Facebook

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

Digital data related to user IDs:

-1279801734

-100023633720499

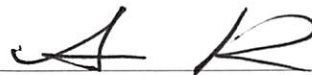
-100002532176517

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

1/31/19

Executing officer's signature

SA Ariana Kroshinsky

Printed name and title



**ATTACHMENT A-2**

**Target Accounts Facebook, Inc.**

1. This warrant applies to information associated with Facebook user IDs:

- a. 1279801734;
- b. 100023633720499; and
- c. 100002532176517

that are stored at the premises owned, maintained, controlled, or operated by Facebook, Inc. located at 1601 Willow Road, Menlo Park, California.

## **ATTACHMENT B -2**

### **Facebook - Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information for the account described in Attachment A-2, is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A-2:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

- of;
- (i) All information about the Facebook pages that the account is or was a “fan”
  - (j) All past and present lists of friends created by the account;
  - (k) All records of Facebook searches performed by the account;
  - (l) All information about the user’s access and use of Facebook Marketplace;
  - (m) The types of service utilized by the user;
  - (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
  - (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
  - (p) All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that relates to the ongoing investigation of violations of 18 U.S.C. § § 241 and 249 (Conspiracy to Violate Civil Rights and Hate Crimes); and 18 U.S.C. § 2261A (Cyberstalking) involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, including, for each user ID identified on Attachment A-2, information pertaining to the following matters:

- (a) Any content including e-mails, messages, texts, photographs, visual images, documents, spreadsheets, address lists, contact lists or communications of any type which could be used to identify the user and or their location;

(b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts;

(c) All subscriber records associated with the specified accounts, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service including any credit card or bank account number;

(d) Any and all other log records, including IP address captures, associated with the specified accounts; and

(e) Any records of communications between Facebook and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

AO 93 (Rev. 11/13) Search and Seizure Warrant

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

FILED ENTERED  
LODGED RECEIVED  
FEB 01 2019 GT  
AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Target Google Accounts, more particularly described in  
Attachment A3

Case No.

MJ18-584 (3)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):

Target Google, Inc. Accounts, user IDs 117906598794476810352 and 114036295919816718188, more particularly  
described in Attachment A3, attached hereto and incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

The information and items set forth in Attachment B3 hereto.

**YOU ARE COMMANDED** to execute this warrant on or before Jan. 4, 2019 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Mary Alice Theiler, United States Magistrate Judge.  
(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)

☐ for        days (not to exceed 30) ☒ until, the facts justifying, the later specific date of 02/03/2019.

Date and time issued: 12/21/2018 at 11:30 AM

  
Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge  
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

## Return

Case No.:

MJ18-584(3)

Date and time warrant executed:

1/4/19, 9:19AM

Copy of warrant and inventory left with:

Google LERS

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Digital data related to Google Inc Accounts  
 117906598794476810352 and  
 114036295919816718188

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date:

1/31/19




Executing officer's signature

SA Ariana Kroshinsky

Printed name and title

**ATTACHMENT A-3**

**Target Accounts Google, Inc.**

1. This warrant applies to information associated with Google user identification numbers and Google + user id #'s:

- a. 117906598794476810352; and
- b. 114036295919816718188

that are stored at the premises owned, maintained, controlled, or operated by Google, Inc., located at 1600 Amphitheatre Parkway, Mountain View, California 94043.



**ATTACHMENT B-3**

**Google - Particular Things to be Seized**

**Section I - Information to be disclosed by Google, for search:**

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Google, including any e-mails, records, files, logs, backup data from third party apps such as WhatsApp, or information that has been deleted but is still available to Google or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

**The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.**



## **Section II - Information to be seized by the government**

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 241 and 249 (conspiracy to violate civil rights or hate crimes); 18 U.S.C. §§ 2261A (Cyberstalking), involving Rodrigue Fodjo Kamden, Christian Fredy Djoko, and Marie Christine Fanyo-Patcho, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

- a. The cyberstalking and harassment of U.M.;
- b. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;
- c. Any address lists or buddy/contact lists associated with the specified account;
- d. All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;
- e. Any and all other log records, including IP address captures, associated with the specified account;
- f. Any records of communications between Google, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.